A Hybrid Tabu Genetic Metaheuristic for Selection of Security Controls

Sarala Ramkumar, Pondicherry Engineering College, Pondicherry, India
Zayaraz Godandapani, Pondicherry Engineering College, Pondicherry, India
Vijayalakshmi Vivekanandan, Pondicherry Engineering College, Pondicherry, India

ABSTRACT
In the modern world, globalization has made way for easy access to information systems for running businesses effectively. The misuse of information systems may lead to loss of productivity, revenue, and sometimes to legal liabilities. Therefore, information security is a major concern for running the business successfully. It is the responsibility of the information security personnel of an organization to develop strategies, and identify the suitable controls to mitigate the risks to which the organization is exposed to. Selection of a suitable set of security controls depends upon, the risks to be addressed, the impact of the risks in terms of revenue, and the cost incurred in implementing the selected controls. To assist in the selection of optimal security controls a hybrid intelligent approach combining the tabu search technique and genetic algorithm has been proposed. The obtained results prove that the proposed approach provides better results in the selection of optimal counter measures.

KEYWORDS
Decision Making, Information Security Risk Assessment, Multi-Objective Optimization, Optimal Security Controls, Tabu-Genetic Hybrid Metaheuristic,

1. INTRODUCTION
Information Systems play a crucial role in the modern digital era. Information systems are considered as corporate assets and securing them has become a major responsibility Ng et al. (2013). The Information Security Breaches Survey (2013, 2014, 2015, 2016, and 2017) by the PwC team has found that the total cost of dealing with security incidents continues to increase year by year. The US Governments Legal Information Institute (US Code Title) defines information security as the means to protect the information assets of an organization from disclosure, modification, and destruction thereby ensuring their confidentiality, integrity and availability. Information security risk management helps in achieving the security goals of an organization. Risk management is fundamental to the security of any organization and helps to assess its security posture. According to the NIST SP 800-39, the information security risk management constitutes a set of activities for identifying risks to the information assets of an organization and provides a mitigation plan that suggests controls to overcome those risks. It aims at identifying the vulnerabilities that exist in the assets, the threats to them, the attacks that may be performed by exploiting the vulnerabilities leading to risks to the organization and the security controls for ensuring safety and security of those assets. The ISO 27002 addresses nearly 133 security controls under the category of technical, operational and administrative controls. There is a need to ensure, whether the security controls in place are effective in securing the

DOI: 10.4018/IJAMC.2019100103

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
information assets of the organization. The verification of the effectiveness of the controls helps in ensuring the security of the assets and hence the security posture of the organization as well.

The selection of suitable security controls based on the security posture of the organization helps not only in running the business successfully, but also helps in maintaining the customer’s confidence and the reputation and public image of the organization. This selection is a multi-objective problem because a best solution set is to be chosen in such a way that it addresses the maximum number of vulnerabilities, is well within the given budget constraints, and also the cost incurred is less than the loss suffered in case of a security breach.

This paper handles the problem of selecting the effective set of security controls by using a hybrid metaheuristic approach that makes use of genetic algorithm (Goldberg, 1989) and tabu search technique (Glover, 1989). The Pareto optimal set of security controls identified by using the tabu search process is taken as the initial population for the genetic algorithm to choose the best population of the global optimal security controls. The effectiveness of the proposed approach is evaluated based on the number of vulnerabilities addressed and cost incurred in the security controls selection. The experimental results obtained are compared based on the generational distance, inverted generational distance and spread parameters used for evaluating the diversity and convergence characteristics of multi-objective optimization algorithms.

The rest of the paper is organized as follows. Section 2 discusses the work done in literature. Section 3 explains the selection of security controls, multi-objective optimization, tabu search, genetic algorithm and the hybridization of metaheuristic algorithms. Section 4 discusses the proposed hybrid tabu genetic approach for countermeasure selection. The experimental results are discussed in section 5 and the conclusion in section 6 respectively.

2. RELATED WORK

Determining the set of security controls that are appropriate and cost effective for a given situation is a complex task as it involves, matching the threats to vulnerabilities, identifying the frequency of the attacks, and mapping between the vulnerabilities to the security controls. The techniques that have been proposed in the literature for solving this multi-objective problem can be classified into defence based approaches and optimization-based approaches. The defence based approaches address from the attacker perspective and use attack countermeasure trees and scenario modelling to decide on appropriate security controls. The optimization-based approaches however focus on the objectives such as cost of security controls, vulnerabilities addressed and residual risks. Economic indicators like return on investment, net present value are also used to find the suitable security controls.

Gupta et al. (2006) proposed an approach where the countermeasure selection was done to minimize the residual vulnerabilities. A genetic algorithm approach is used for implementing a set of security controls by matching information security vulnerabilities to organizational security profiles. But a generic set of vulnerabilities and security controls are considered instead of identifying the proper security controls for the actual vulnerabilities that exist in the organization. Bistarelli et al. (2007) proposed a qualitative approach for the selection of security controls to protect an IT system from attacks. Security scenarios are modelled using defence trees and the countermeasure selection is done using conditional preference networks. The administrator’s preferences are given, and a preference table is constructed which is used for inference. There is no exact matching between the vulnerabilities and countermeasures. Also, a single countermeasure can overcome multiple vulnerabilities. This is not considered in the construction of the defence trees with their leaves as countermeasures.

Ojamaa et al. (2008) proposed a hybrid expert system for optimal selection of security controls. This expert system enables the user to select a countermeasure in a rational way based on the Pareto optimality computation using discrete dynamic programming by taking into account the available resources. Nagata et al. (2009) proposed a fuzzy outranking based approach for selecting risk mitigation controls. The security controls are compared using a fuzzy relation called outranking and the critical
Related Content

Nature-Inspired-Based Adaptive Neural Network Approximation for Uncertain System
www.igi-global.com/chapter/nature-inspired-based-adaptive-neural-network-approximation-for-uncertain-system/190171?camid=4v1a

Gene Clustering Using Metaheuristic Optimization Algorithms
www.igi-global.com/article/gene-clustering-using-metaheuristic-optimization-algorithms/132522?camid=4v1a
Theorems Supporting r-flip Search for Pseudo-Boolean Optimization
www.igi-global.com/chapter/theorems-supporting-flip-search-pseudo/63816?camid=4v1a

A Technique to Exploit Free-Form Notes to Predict Customer Churn
www.igi-global.com/article/a-technique-to-exploit-free-form-notes-to-predict-customer-churn/103267?camid=4v1a